Contribution ID: **3**

Type: **Talk**

AI model for securing Internet of Things communication systems in smart agriculture.

Wednesday, 3 July 2024 13:20 (20 minutes)

The rapid increase of Internet of Things (IoT) devices in smart agriculture has enabled a more connected and intelligent world. IoT devices are a collection of interconnected systems that can communicate, share data and information to achieve an automated environment. Smart agriculture presents a transformative approach to farming that leverages technology and data-driven solutions to address the challenges of modern agriculture, including the need to sustain a growing global population while minimising environmental impact and resource depletion. However, the increase in the deployment of IoT systems has led to an increase in cyber-attacks and security challenges. Moreover, security challenges such as man-in-the-middle, denial and distributed denial of service, botnets, sinkhole and spoofing attacks compromise the confidentiality, integrity and availability (CIA) of smart agriculture. This study investigates measures deployed for anomaly detection and prevention in IoT smart agriculture communication systems. Furthermore, the study proposes a model that incorporates machine learning techniques to identify and predict anomalies in loT communication systems and adapt security measures dynamically. Python is used to develop the proposed model and tested on accuracy, recall, f1-score, precision, true positive rate, false positive rate metrics. The IoT-based Datasets CIC-IDS2018, ToN-IoT and Edge-IIoTset are used to evaluate the performance and efficiency of the proposed model.

Primary authors: NGOMANE, Issah (University of Mpumalanga); BEMBE, Mncedisi (University of Mpumalanga); Prof. VELEMPINI, Mthulisi (University of Limpopo)

Presenter: NGOMANE, Issah (University of Mpumalanga)

Session Classification: Session